

1 REMARKS

2 Claims 1-3, 5-7, 10, 11, 13, 14, 16-22, 25-27, 29, 31, 34-50, 58, and 59  
3 have been amended.

4 Claims 1-66 are pending

5  
6 Rejections

7 **Claims 1-66** stand rejected under 35 U.S.C. §102(b) as being anticipated by  
8 U.S. Patent No. 4,835,682, issued to Kurachi et al (hereinafter referred to as  
9 *Kurachi et al*). Applicants respectfully disagree with the rejections for at least the  
10 following reasons.

11 *Kurachi et al.* disclose techniques for preventing unauthorized copying of  
12 software programs stored on floppy drives. To do this, *Kurachi et al.* take  
13 advantage of a floppy disk controller/drive that supports two different frequency  
14 modulation modes, namely a standard frequency modulation (FM) mode and a  
15 non-standard frequency modulation mode (MFM). *Kurachi et al.* also utilize a  
16 machine ID associated with the host computer that is attempting to load a program  
17 that is stored on a floppy disk using the MFM mode. In order to read the floppy  
18 disk, the host computer is required and configured to convert the MFM written  
19 program and rewrite it to the floppy disk using the FM mode. During the rewrite  
20 to the floppy disk, the program is modified based on the machine ID such that  
21 when the floppy disk is read in the future only the host computer will be allowed  
22 to run the modified program stored on the floppy disk. *Kurachi et al.* teach that  
23 the modified program is de-modified and the resulting original program is then  
24 allowed to run. If the rewritten floppy disk is subsequently inserted into another  
25

1 computer having a different machine ID, the program cannot be de-modified and  
2 therefore cannot be run.

3 **Independent Claim 1**, is drawn to a method that includes having at least  
4 one computer receive unique key data from at least one other computer. The at  
5 least one computer then converts the initial digital good into a modified digital  
6 good using the unique key data to selectively individualize the initial digital good  
7 for use with the computer, such that the modified digital good has a substantially  
8 unique operative configuration that properly functions with the computer. The  
9 method also includes causing the at least one computer to run the modified digital  
10 good. *Kurachi et al.* fail to disclose or reasonably suggest a modified digital good,  
11 which while customized for use on a given computer, can be run. Instead,  
12 *Kurachi et al.* teach that their modified program is de-modified and the resulting  
13 original program is then allowed to run. Here, in accordance with certain aspects  
14 of the present invention, the modified program is unique in its operative  
15 configuration for the given computer and runs.

16 **Claim 2**, which depends from Claim 1, further specifies that the conversion  
17 act further includes manipulating at least one flow control operation within the  
18 initial digital good. *Kurachi et al.* fail to disclose or reasonably suggest the notion  
19 of manipulating the flow control of the program. Indeed, *Kurachi et al.* teach that  
20 their modified program needs to be de-modified to reproduce the resulting original  
21 program.

22 **Claim 3**, which depends from Claim 1, further specifies that at least one  
23 other computer generates the unique key data based on at least one unique  
24 identifier data associated with the computer. *Kurachi et al.* fail to disclose or  
25

1 reasonably suggest having another computer generate any key data. Indeed,  
2 *Kurachi et al.* teach that the computer uses its own internal machine ID.

3 **Claim 4**, which depends from Claim 3, further specifies that the method  
4 allows for selective limitations on the operation of the modified digital good to  
5 computers that are properly associated with at least the unique identifier data.  
6 *Kurachi et al.* fail to disclose or reasonably suggest having other properly  
7 associated computers run the program. Indeed, *Kurachi et al.* teach that only the  
8 computer can run their de-modified program.

9 **Claim 5**, which depends from Claim 3, further specifies that the method  
10 includes causing the at least one computer to provide the unique identifier data  
11 associated with the at least one computer to the at least one other computer, and  
12 causing the at least one other computer to cryptographically generate the unique  
13 key data based on the unique identifier data provided by the at least one computer  
14 and at least one secret key. *Kurachi et al.* fail to disclose or reasonably suggest  
15 having the computer provide unique identifier data to other computers or having  
16 other computers cryptographically generate unique key data based as recited in  
17 Claim 5. Indeed, *Kurachi et al.* teach that the computer can use its machine ID to  
18 verify if the de-modified program (i.e., their original program) can be run.

19 **Claim 6**, which depends from Claim 3, further specifies that the at least one  
20 other computer generates at least a first key and a second key, and the first key and  
21 the second key are different, but cryptographically related to the secret key, and  
22 wherein the received unique key data includes the first key. *Kurachi et al.* fail to  
23 disclose or reasonably suggest having another computer generate multiple related  
24 cryptography keys based in part on provided unique identifier data. Indeed,  
25 *Kurachi et al.* are silent when it comes to cryptography and key generation,

1 especially when their computer simply uses its machine ID to modify the program  
2 and later de-modify the program so it can be run in its original configuration.

3 **Claim 7**, which depends from Claim 1, recites that the method further  
4 includes dividing the initial digital good into at least a first portion and a second  
5 portion using the at least one other computer, providing the first portion to the at  
6 least one computer via a first computer readable medium, and subsequently  
7 providing the second portion to the at least one computer via a second computer  
8 readable medium. *Kurachi et al.* fail to disclose or reasonably suggest having  
9 another computer divide their original program and provide them portions using at  
10 least two mediums. Instead, *Kurachi et al.* focus only on the delivery of their non-  
11 standard frequency modulation mode (MFM) written program on a floppy drive.

12 **Claim 8**, which depends from Claim 7, further recites that the first  
13 computer readable medium includes a different type of computer readable medium  
14 than the second computer readable medium. Again, *Kurachi et al.* focus only on  
15 the delivery of their MFM written program on a single two-sided floppy drive.

16 **Claim 9**, which depends from Claim 8, further recites the first computer  
17 readable medium includes a fixed computer readable medium and the second  
18 computer readable medium includes a network communication. As before, Again,  
19 *Kurachi et al.* focus only on the delivery of their MFM written program on a  
20 single two-sided floppy drive.

21 **Claim 10**, which depends from Claim 7, further recites that the method  
22 includes having the at least one other computer convert the second portion into a  
23 modified second portion using the unique key data to selectively manipulate at  
24 least one flow control operation within the second portion, such that the modified  
25 second portion is operatively different in configuration to the second portion, and

1 providing the modified second portion to the at least one computer via the second  
2 computer readable medium. *Kurachi et al.* fail to teach these additional features.

3 *Kurachi et al.* also fail to teach the additional features recited in the  
4 following claims: **Claim 11**, which depends from Claim 10, further recites that the  
5 at least one other computer is used to convert the second portion into the modified  
6 second portion. **Claim 12**, which depends from Claim 10, further recites that the  
7 unique key data includes at least a first key and a second key, and converting the  
8 second portion into a modified second portion further includes using the second  
9 key to selectively manipulate at least one flow control operation within the second  
10 portion. **Claim 13**, which depends from Claim 10, further recites that the unique  
11 key data includes at least a first key and a second key, and that providing the  
12 second portion to the at least one computer further includes providing the first key  
13 to the at least one computer. **Claim 14**, which depends from Claim 13, further  
14 recites that the at least one computer converts the first portion into a modified first  
15 portion using the first key to selectively manipulate at least one flow control  
16 operation within the first portion, such that the modified first portion is operatively  
17 different in configuration, and that the at least one computer operatively combines  
18 the modified first portion and the modified second portion to produce the modified  
19 digital good. **Claim 15**, which depends from Claim 13, further recites selectively  
20 limiting operation of the modified digital good to computers that are properly  
21 associated with at least the first key.

22 **Claim 16**, which depends from Claim 3, recites that the method further  
23 includes having the at least one computer to provide the unique identifier data  
24 associated with the at least one computer to the at least one other computer, and  
25 accessing computer identification data within the at least one computer and

1 including the computer identification data within the unique identifier data  
2 associated with the at least one computer. **Claim 17**, which depends from Claim  
3 16, further specifies receiving user identification data at the at least one computer  
4 and including the user identification data within the unique identifier data  
5 associated with the at least one computer. While *Kurachi et al.* teach that machine  
6 IDs can be used within open computer, they fail to teach that other data may be  
7 used and/or that user identification data can be received and included in the unique  
8 identifier data that is provided to the other computer.

9 Consequently, claims 1-17 are patentable over *Kurachi et al.*

10 The remaining claims will be summarized as they share at least some of the  
11 same novel differences as one or more of the claims presented above. Here,  
12 **Independent Claim 18** recites a computer that receives an initial digital good and  
13 unique key data from at least one other computer, and converts the initial digital  
14 good into a modified digital good using the unique key data to selectively  
15 individualize the initial digital good for use with the at least one computer, such  
16 that the modified digital good has a substantially unique operative configuration  
17 that properly functions with the computer. *Kurachi et al.* fail to teach this claimed  
18 invention. **Claims 19-26**, which depend at least in part on Claim 18, recite further  
19 limitations similar to Claims 2-17. Again, *Kurachi et al.* fail to teach these  
20 claimed inventions. Hence, Claims 18-26 are patentable over *Kurachi et al.*

21 **Independent Claim 27** is directed towards a computer-readable medium  
22 comprising computer-executable instructions for receiving unique identifier data  
23 associated with at least one computer, generating unique key data based on at least  
24 the unique identifier data, converting at least a portion of an initial digital good  
25 using the unique key data to selectively individualize the portion of the initial

1 digital good, such that a modified portion of the digital good is produced that is  
2 operatively different in configuration, and providing at least the modified portion  
3 of the digital good and at least a portion of the unique key data to the at least one  
4 computer. For at least the reasons described above, Claim 27 is patentably distinct  
5 from *Kurachi et al.* Depending from Claim 27 and adding still further novel  
6 limitations are **Claims 28-33**, each of which is patentable too over *Kurachi et al.*  
7 for at least the reasons presented above.

8 **Independent Claim 34** is directed towards an apparatus for use in a host  
9 computer. The apparatus includes an individualizer that is configured to receive  
10 unique key data and at least a portion of an initial digital good from at least one  
11 source computer, and produce at least a portion of a modified digital good using  
12 the unique key data to selectively individualize the initial digital good for use with  
13 the host computer, and such that the modified digital good is operatively different  
14 in configuration than the initial digital good. For at least the reasons described  
15 above, Claim 34 is patentably distinct from *Kurachi et al.* Depending from Claim  
16 34 and adding still further novel limitations are **Claims 35-42**, each of which is  
17 patentable too over *Kurachi et al.* for at least the reasons presented above.

18 **Independent Claim 43** recites an apparatus for use in a source computer.  
19 Here, the apparatus includes a key generator that is configured to receive a unique  
20 identifier data from a destination computer and generate unique key data based on  
21 the received unique identifier data associated with the destination computer. The  
22 apparatus also includes an individualizer configured to receive the unique key data  
23 and at least a portion of an initial digital good and output at least a portion of a  
24 modified digital good using the unique key data to selectively individualize the  
25 initial digital good, such that the modified digital good is operatively different in

1 configuration than the initial digital good. For at least the reasons described  
2 above, Claim 43 is patentably distinct from *Kurachi et al.* Indeed, *Kurachi et al.*  
3 fail to have there source computer and destination computers communicate at all.  
4 Depending from Claim 43 and adding still further novel limitations are **Claims 44-**  
5 **49**, each of which is patentable too over *Kurachi et al.* for at least the reasons  
6 presented above.

7 **Independent Claim 50** recites a system that includes an identifier  
8 configured to output unique identifier data associated with a computer, a key  
9 generator coupled to receive the unique identifier data and generate at least one  
10 unique key data based on the received unique identifier data, and at least one  
11 individualizer configured to receive the unique key data and at least a portion of an  
12 initial digital good and output at least a portion of a modified digital good using  
13 the unique key data to selectively individualize the initial digital good, such that  
14 the modified digital good is operatively different in configuration than the initial  
15 digital good. For at least the reasons described above, Claim 50 is patentably  
16 distinct from *Kurachi et al.* Depending from Claim 50 and adding still further  
17 novel limitations are **Claims 50-66**, each of which is patentable too over *Kurachi*  
18 *et al.* for at least the reasons presented above.

19 Thus, as illustrated in the examples above, Claims 1-66 are each patentable  
20 over *Kurachi et al.* Consequently, it is respectfully requested that the rejections be  
21 reconsidered and withdrawn.



1 Conclusion:

2 The pending claims are clearly patentable over the cited art.

3  
4 Respectfully Submitted,

5  
6 Dated: 9/30/02

7 By: Thomas A. Jolly

8 Thomas A. Jolly  
9 Reg. No. 39,241  
10 (509) 324-9256  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25